Nebraska Information Technology Commission

Government Technology Collaboration Fund - 2001

Grant Application Form

(Deadline for Submission: August 31, 2001)

For more information about Government Technology Collaboration Fund grants, see the Grant Guidelines at http://www.nitc.state.ne.us/sgc/grants/.

Contact information for questions regarding this form:
Rick Becker
Office of the NITC
521 S 14th Street
Lincoln, NE 68508
(402) 471-7984
rbecker@cio.state.ne.us

Enterprise Security Awareness Training Grant

Table of Contents

Section I: General Information

A. Project Title: **Enterprise Security Awareness Training Grant**

Submitting Agency (or Agencies): **Information Management Services Division**
Department of Administrative Services

Contact Information for this Project

Name: **Steve Henderson**
Address: **501 S. 14th St**
City, State, Zip: **Lincoln, NE 68508**
Telephone: **(402) 471-4861**
E-mail: **shenders@notes.state.ne.us**

B. Certification for Request

I certify that to the best of my knowledge the information in this application is correct and that the application has been authorized by this entity to meet the obligations set forth in this application.

Name: **Steve Henderson**

Title: **Acting Administrator**

Agency: **DAS -- IMServices**

Date: **August 31, 2001**

Total Grant Funds Requested: $36,620

Total Project Costs: $93,620

Section II: Executive Summary

Provide a one or two paragraph summary of the proposed project. This summary will be used in other externally distributed documents and should therefore clearly and succinctly describe the project and the information technology required.

In January, 2000, the Nebraska Information Technology Commission (NITC) adopted the first statewide E-government Strategic Plan, which was later endorsed by the Governor. It was stated in this document that security was a priority of the State at an Enterprise level. The NITC Security Architecture Workgroup developed 7 policies, one of which addresses Education, Training, and Awareness. It is stated in this policy that all State employees and other State agents need to be aware of their responsibility towards Security.

The Federal Government is also beginning to mandate certain security steps be taken before states and other organizations can use certain data. The Health Insurance Portability and Accountability Act (HIPAA) has issued five rules. The State of Nebraska has until February, 2003, to comply with the Security and Privacy Rule. Although this seems far into the future, the items listed in this rule will take time to implement.

Funding is needed for a Security Awareness training program to occur at an Enterprise level. Some initial plans are being developed for the initial Rollout of this program. This grant will fund some initial training and will provide a Security Consultant to assist the Security Officers as they attempt to understand Security in their Agencies, Boards, and Commissions.

Section III: Goals and Objectives

1. Describe the project, including the specific goals and objectives.

2. Describe the project's relationship to the agency's comprehensive technology plan.

3. Describe, if applicable, how this project furthers the implementation of electronic government. [Preference will be given to projects which support the State Government Council's priority of implementing electronic government as reflected in the goals of the Business Portal Action Plan and the E-Government Strategy (available at http://www.nitc.state.ne.us/sgc/).]

As the State's computer networks are opened to more users through the use of E-government, the needs for security awareness are going to increase. The NITC's Security Architecture Workgroup has issued Security policies that state the importance of training to security. The Federal government is beginning to mandate that Security Awareness Training be available for State employees and others who access data of various types. The Health Insurance Portability and Accountability Act (HIPAA) requires that training and other security requirements be met by February, 2003.

The goal of this grant is to provide the State with a means to educate State employees about the importance of computer security. To begin to address the Security Policy and HIPAA rules, plans are being developed for statewide Security Training. This program would include:

- Naming the Security Officers in the State's Agencies, Boards, and Commissions,
- Initial Roll-out training for the Security Officers,
- Training for Information Systems Technical Personnel, and
- Training for other State employees.

Funding of this grant would cover costs associated with this training, including development of training materials, training time, and consultation after the training. As part of the initial rollout of this training program, approximately 110 Security Officers and 950 State employees would be trained through this grant. IMServices employees who are specialists in the computer security area would perform the Training.

Section IV: Scope and Projected Outcomes

Describe the project's specific scope and projected outcomes. The narrative should address the following:

1. Beneficiaries of this project and the need(s) being addressed;

2. Expected outcomes of the project;

3. Measurement and assessment methods that will verify project outcomes;

Beneficiaries and Needs Addressed by Project

The NITC's Security Architecture Workgroup has outlined several policies (see www.nitc.state.ne.us/tp/workgroups/security/security_policies.htm for more information) they feel need to be addressed to ensure that the State maintains a minimal level of security on its computers and networks. One of these policies regards Education, Training, and Awareness. The objectives of this policy include:

1. To communicate responsibilities for the Education, Training, and Awareness of information security policies and procedures;
2. To provide adequate skills for technical staff responsible for implementing security procedures;
3. To establish specific requirements for achieving the goals of Education, Training, and Awareness; and,
4. To communicate the consequences of violations of security procedures.

Five HIPAA rules have been published to date, with the Security and Privacy rule mandated to be in place by February, 2003. Part of this rule requires that anyone having access to computers or to the data related to HIPAA be aware of the need for security, know what it means to them, and know what the consequences are should the security be breached.

The funding of this training will allow the State to comply with this HIPAA rule and address the issues in the Security Policy. It will also enable the State to train staff from the various Agencies, Boards, and Commissions so that a minimal level of security can be maintained Statewide. This is especially needed since the State is utilizing E-government more each day. As more of the State's computers and networks are accessed from the Internet, the security of data and programs needs to be maintained, even as technology changes.

Expected Outcomes of Project

Computer security is an Enterprise concern. If an employee at any level misuses the data or access to it, the entire State government is at risk to some extent. This grant will provide training for a Security Officer in each Agency, Board, and Commission. This person will then be able to inform others in their organization about the State's security guidelines. The Security Officer would also be informed of the Security enforcement guidelines and the actions that should be taken if a security breach occurs.

Each Agency, Board, and Commission will name a Security Officer for their organization. This person will attend a 4-hour class regarding computer security. A Security Manual will be provided to the Security Officers that outlines the State's expectations on Security, how it should be maintained, guidelines to follow, and what should be done if a Security breach of any sort is discovered.

Other State employees also need security training. The grant will fund a 2-hour security training class for approximately 850 employees. There will be two versions of this class – one for general computer users and one for IS Technical staff. This class will inform the employees of their responsibilities towards computer security.

The funding of this grant will allow the materials to be developed and distributed, and will provide funding for the trainer of the class. Should there be security questions or concerns, this grant will also fund a Security Consultant for approximately 1 year. It is expected that all the classes will be scheduled within approximately 1 year of the funding of this grant.

Measurement and Assessment Methods of Project

This project will have three basic components – training of Security Officers, training of general and computer users, and consultation. The two training components can be measured by keeping a record of attendees in the classes. The Security Officer training will have approximately 6 classes with between 5 and 20 attendees in each class. Each class would last about 4 hours. This will allow for greater interaction between the participants and a greater transfer of knowledge. These classes will be scheduled within the first 6 months of the funding of this grant.

The general user and IS Technical Staff training will be provided for other State employees. This training would be provided to approximately 450 IMServices employees and contractors, as well as 500 employees from other Agencies, Boards, and Commissions who wished to have their employees receive the training. There would be up to 40 of these classes, with each class lasting about 2 hours. The size of these classes would depend on the facilities that were available to hold the training. These classes will all be scheduled within approximately 1 year of the funding of this grant.

A Security Consultant position will also be funded for approximately 1 year. This can be measured through the questions that are asked, and the time it takes to address the issues presented.

Section V: Project Justification / Business Case

Please provide the project justification in terms of tangible benefits (an economic return on investment) and/or intangible benefits to the agency or the public. The narrative should address the following:

1. Tangible: Economic cost/benefit analysis;

2. Intangible: Benefits of the project for customers, clients, and citizens and/or benefits of the project for the agency;

3. Other solutions that were evaluated and why they were rejected. Include their strengths and weaknesses. Explain the implications of doing nothing and why this option is not acceptable;

4. If the project is required to comply with a state or federal mandate, please so indicate.

Cost/Benefit Analysis

Cost	Benefit	Projected Savings
1. The cost of this project to the State of Nebraska is projected to be $93,620.	The State will be provided with Security Officers that will be able to monitor and enforce Security guidelines. In addition, approximately 950 State employees and contractors will be educated as to their responsibilities towards Security.	If an employee was not aware of the need for confidentiality with regards to data they were processing (i.e., Social Security Numbers, medical records, disciplinary actions, etc.), and data was released to the general public, the various news media could be informed of the situation. The State could spend upwards from $1,000,000 for investigations and lawyers. In addition, public relations specialists would be needed to address the situation. State employees would also be informed of the need to report security breaches quickly, which will also help to minimize the costs should a breach occur.

2. The costs of this project to IMServices and other State Agencies, Boards, and Commissions will be in terms of labor.	It is very important that State employees who deal with confidential data or who have Internet access understand their responsibilities with regards to computer security.	Training employees about their responsibilities towards security can save the State much effort and money by preventing security breaches before they occur. If employees are trained, they may also be able to report a security breach sooner, limiting any damage that may occur.
3. Funding a Security Consultant could help all the State Agencies, Boards, and Commissions be assured that they are taking necessary steps to protect their data and networks.	Many of the State's Agencies, Boards, and Commissions do not have the resources to have their own Security Consultant. This will make the same expertise available to all Agencies, Boards, and Commissions, regardless of their size or budget.	Keeping the State's computers and networks safe from unauthorized access is a priority of the NITC's Security Architecture Workgroup. This will support that effort without having to hire outside security consultants. It will make the most of the State's limited resources.
4. Training a Security Officer for each Agency, Board, and Commission will be a large endeavor.	Having multiple Security Officers spread throughout State government will help ensure that the State's data and networks are kept safe. This will allow a higher exposure of State employees to the security issues.	Increasing the exposure and understanding of security will help everyone understand its importance. Employees will have a higher awareness of their responsibility, and that will help to safeguard the data that is stored on the State's computers.

Other solutions and why rejected

There are numerous ways of having the State's employees trained with regards to their responsibilities in Computer Security. Many of those efforts would require more money by hiring outside Security Consultants. The consultant could also be the single source of expertise for the State.

This approach allows each Agency, Board, and Commission to have their own expert who is trained in computer security. That expert will have documents they can use to assist them. Should the documents not be sufficient, there will also be a part-time security consultant funded that can offer more assistance beyond the training.

The Security Officers will have the option of doing the initial training of their staff themselves, or of sending the staff members to training that is funded by this grant. This will derive the maximum amount of benefit out of the limited resources available to the State, and still begin preventing security breaches as soon as possible.

State Mandate -- NITC Goals Initiated by Governor

In the NITC's E-Government Strategic Plan, it was noted that an enterprise approach is essential for statewide security. To address the need for security, the NITC commissioned a Security Workgroup to create policies to help guide the State as E-government was developed. One of the policies created states the need for Security Awareness Training for State employees at all levels.

This grant will fund the initial rollout of this training so that a minimal level of security awareness can be ensured throughout State government. An enterprise approach to this training will also enable the various Agencies, Boards, and Commissions to have the same understanding of the importance of security, and why everyone should be responsible for it.

Federal Mandate -- HIPAA Security and Privacy Rules

The Health Insurance Portability and Accountability Act (HIPAA) has issued a rule that certain security and privacy rules will be implemented by February, 2003. Part of this policy states that all employees, agents, and contractors must participate in a Security Awareness Training program. It also states that there needs to be a Security Management process that includes the establishment of accountability, management controls, and penalties for the abuse and misuse of the State's assets.

The State of Nebraska would need to develop a program to address these issues. Since they would need to be enforced over a large section of State government to comply with HIPAA, it seems reasonable to ensure that all data is secure by having the same rules apply to all of State government. If employees should move between positions, they would already have a basic knowledge of their responsibility for security, and the importance that the State places on this responsibility.

Section VI: Implementation

Describe the implementation plan -- from design through installation and ongoing support -- for the project. The narrative should address the following:

1. Project sponsor(s) and stakeholder acceptance analysis;
2. Define the roles, responsibilities, and required experience of the project team;
3. List the major milestones and deliverables for each milestone;
4. Training and staff development requirements and procedures;
5. Ongoing support requirements, plans and provisions.

Stakeholder acceptance analysis

The sponsor of this project would be Steve Henderson, Acting Administrator for IMServices. The primary stakeholders for this project would be the NITC, the NITC Security Architecture Workgroup, and IMServices.

In its E-Government Strategic Plan, the NITC recognized the need for an Enterprise approach to security. In the Strategic Plan, they stated that effective measures need to be taken to assure that security and privacy is maintained. The NITC Security Architecture Workgroup developed 7 policies towards security, one of them focusing on Education, Training, and Awareness of Security issues. The objectives of this policy include:

1. To communicate responsibilities for the Education, Training, and Awareness of information security policies and procedures;
2. To provide adequate skills for technical staff responsible for implementing security procedures;
3. To establish specific requirements for achieving the goals of Education, Training, and Awareness; and,
4. To communicate the consequences of violations of security procedures.

In order to address these objectives Statewide, a training program needs to be established that will provide the same training to all Agencies, Boards, and Commissions. The best way to accomplish this is to have each organization name a Security Officer, train that person, and then offer additional training to other employees. The funding of this grant would provide an initial rollout of this training.

This project is also mandated by HIPAA security and privacy rules. It is important that the gaps identified in the MMIS/HIPAA Security Gap Analysis document is met prior to the federal deadlines. IMServices and Health and Human Services have a strong interest to ensure compliance so that Federal funding will continue and fines will not be imposed. Taking an enterprise approach to this issue will not only help the State to comply with the requirements, but will also benefit the rest of State government.

Roles, responsibilities, and required experience of project team

This grant would fund the time for security specialists to provide training to Security Officers and other State employees. These specialists would need to have an understanding of all aspects of security, including the need for physical security, logon security, data confidentiality, and enforcement of security policies. These security specialists will develop the curriculum that will be used in the training, and ensure that everyone attending the training receives documentation that can be referred to after the training.

Since questions regarding security will arise, a security consultant position is also being funded by this grant. This person will also be a security specialist, and needs to be familiar with the training that was performed. This security specialist could be one of the trainers that performed the training.

Milestones and deliverables

Following is a list of milestones and deliverables from this project.

Milestones	Deliverables
1. Identify Security Officers in each Agency, Board, and Commission	List of Security Officers that will be invited to the Security Officer training
2. Finalize curriculum for the Security Officer training, General User training, and IS Technical Staff training.	Have class agendas finalized. Be able to duplicate and distribute class materials.
3. Identify Security Consultant(s).	Be able to identify Security Consultant(s) in training sessions.
4. Schedule Security Officer training. Invite Security Officers to attend.	Have list of which Security Officers are attending which session.
5. Schedule IS Technical Staff Training for IMServices employees.	Have list of which employees are attending which session.
6. Schedule additional General User and IS Technical Staff Training sessions. Coordinate with Agencies, Boards, and Commissions to have State Employees invited	Have list of which employees are attending which session.

Training and staff development requirements and procedures

The trainers will be using the Security documents that are being finalized to develop their class agendas. They will reference the Security Officer Guide, the IS Technical Staff Handbook, and the Computer User's Security Handbook in their classes. The Security Consultant(s) will also need to be very familiar with these documents.

Ongoing support requirements and provisions

This grant will cover the initial rollout of this project. The NITC's Security Architecture policy does state that additional and periodic training is needed. The additional training can be accomplished in many inexpensive ways. Agencies, Boards, and Commissions may decide how best to handle this for their organizations.

Section VII: Technical Impact

Describe how the project enhances, changes or replaces present technology systems, or if new systems are being added. The narrative should address the following:

1. Descriptions of hardware, software, and communications requirements for this project. Describe the strength and weaknesses of the proposed solution;

2. Issues pertaining to reliability, security and scalability;

3. Conformity with applicable NITC technical standards and guidelines (available at http://www.nitc.state.ne.us/standards/) and generally accepted industry standards;

4. Compatibility with existing institutional and/or statewide infrastructure.

This grant is for Enterprise Security training only so there are not many technological requirements. The training would address the issues outlined in the NITC's Security Architecture Education policy, and would provide the basis for meeting the HIPAA Security Training and Management Process rules.

Section VIII: Risk Assessment

Describe possible barriers and risks related to the project. The narrative should address the following:

1. List the identified risks, and relative importance of each;

2. Identify strategies which have been developed to minimize risks.

There are not many risks associated with this grant since it is not a technological issue. Most of the risks are associated with NOT providing Security Awareness training. If this training is followed, the employees of the State of Nebraska should have the information that is needed to follow the Security Policies as issued by the NITC's Security Architecture Workgroup. This will allow the State of Nebraska to partially comply with the HIPAA requirements on Security and Privacy.

Section IX: Financial Analysis and Budget

1. Provide the following financial information:

	GTCF Grant Funding	Cash Match	In-Kind Match	Other Funding Sources	**Total**
Personnel Costs	$30,770 (1)		$57,000 (3)		
Capital Expenditures (Hardware, software, etc.)					
Contractual Services					
Supplies and Materials	$5,850 (2)				
Telecommunications					
Training					
Travel					
Other costs					
Total	$36,620	❶	$57,000 ❷		$93,620 ❸

2. Provide a detailed description of the budget items appearing above.

Item (1) Personnel Costs (GTCF Grant Funding)
This item will provide funding for the time to develop training materials, and the time of the trainers to train the Security Officers. Each session is anticipated to be about 4 hours in duration, with about 6 classes being held. It is also anticipated that it will take about 40 hours for the training agenda to be developed.

4 hours x 6 sessions x $85/hr = $2040
40 hours x $85/hr = $3400

Total = $5,440

There would also be additional training time for the training of IMServices employees and employees from other State entities. It is anticipated that each of these sessions will last approximately 2 hours, and that there would be approximately 40 of these sessions held. It would take approximately 10 hours to develop the training agenda for these sessions.

2 hours x 40 sessions x $85/hr = $6,800
10 hours x $85/hr = $850

Total = $7,650

This grant would also cover the time for a person to act as a Security Consultant to the Agencies, Boards, and Commissions. It is anticipated that this endeavor would take approximately 10% of 1 person's time over a 1-year time period.

208 hours x $85/hr = $17,680

Total Personnel Expenses -- $5,440 + $7,650 + $17,680 = $30,770

Item (2) Supplies and Materials (GTCF Grant Funding)
The manuals for the Security Officer classes are estimated to be approximately $10 for each manual for materials, duplication and assembly. It is anticipated that some Agencies, Boards, and Commissions may want to send more than one person to these sessions. It is estimated that approximately 110 manuals will be needed.

The manuals for the employees of IMServices and other State Agencies, Boards, and Commissions are estimated to cost approximately $5 for each manual for materials, duplication and assembly. There are approximately 450 IMServices employees and contractors. It is anticipated that other agencies may want to have their employees involved in this training. About 500 other State employees are anticipated to be involved in this training.

110 Security Officers x $10/manual = $1100
950 employees x $5/manual = $4,750

Total costs for manuals = $1100 + $4750 = $5,850

Item (3) Personnel Costs (In-Kind Match)
This item would cover the cost of having the 450 IMServices employees and contractors given Security training, as well as 500 additional State Employees given appropriate training.

950 employees x 2 hours/employee x $30/hr/employee = $57,000

Match Requirement

3. Match Requirement: This grant requires a 25% match from the agency. Please use the calculation below to ensure your application meets this requirement.

$$\frac{\text{Total Cash Match } ❶ + \text{Total In-Kind Match } ❷}{\text{Total Project Cost } ❸} \quad \$ \quad 0.25$$

$57,000 / $93,620 = 61%